Five Faulty Assumptions Small Business Owners Make about IT

If you manage a small business, you probably have a broader-than-average list of things to worry about than a typical corporate professional does. However, there are a few IT-related assumptions that, left unchecked, can turn into urgent crises.

Do any of these statements sound familiar?

1. *PCs are throwaway items, so I don't need to repair them.*
2. *I'm too small for anyone to want my data. I don't need to spend money on security.*
3. *I can take care of things myself.*
4. *I haven't had a problem for years. Why should I worry about it now?*
5. *It's too expensive.*

Even if you think you're covered, you may be surprised to discover that there's a cost or security exposure. Ask your IT support resource for more details.

Assumption #1: PCs are throwaway items, so I don't need to repair them.

Over decades, IT hardware has decreased dramatically in price. Hardware is much less expensive (relative to speed and processing power) than it was ten years ago. This leads to the idea that you can measure the business value of a device based solely on its replacement cost.

FACT: Your email and applications are costly to switch, in terms of licenses, installation, migration, and adoption curve.

95% of STS service tickets are *software*-related, not hardware.

In addition, your data is not replaceable. Even if your mission critical data is not stored on a PC, but rather in a cloud application (Google Drive or Microsoft OneDrive, for example), you'll have to re-import data. Not to mention, you'll need to reload client applications.

You'll also need to install and update operating systems; setup and re-enable security; import your preferences; re-map drives and printers, and so on.

These processes can take an inexperienced person an entire day, at a true rolled-up cost (labor, missed business opportunities, unhappy or lost customers) that might exceed the cost of managed IT services for an entire year.

Assumption #2: I'm too small for anyone to want my data. I don't need to spend money on security.

You look at the total size of your operation and wonder, "We have nothing to steal. We're not a target. I'm sure we're under the radar."

FACT: While it is true that highly publicized hacks (Target, Amazon, Google, etc.) are targeted, 99% of hacks occur for no other reason than simply because you are connected to the internet.

Most viruses and malware come through email. You use email, right? A virus or malware does not care how big or small you are.

Depending on the infection, an attack could require a total rebuild. This means spending days to resolve the situation and recover your data if possible. A malware attack could be worse: the mind behind it could encrypt all of your data and demand a costly "ransom" to return it to you.

Common Attacks

- Web-based (browser)
- Phishing or social engineering
- General malware
- SQL injection
- Compromised or stolen device
- Denial of service
- Advanced malware / zero day attack
- Malicious insider
- Cross-site scripting
- Ransomware

Source: Small Business Trends, "Cyber Security Statistics: Numbers Small Businesses Need to Know," January 3, 2017

43% of cyber attacks target small business.*

Here's what you have that cyber criminals want:

1. Customer email addresses and physical addresses
2. Phone numbers
3. Billing addresses
4. Credit card information
5. Asset information
6. Purchase records

If someone walked through the door and asked for this information, you would quickly escort them out. This is why you hire IT security. Security costs a degree of effort and money, but it is far less costly than several days' worth of downtime or a total data disaster.

Assumption #3: I can take care of things myself.

You only have a couple dozen individual user devices in house. You trust your employees to be careful, and some of them are using personal devices. All your key applications and data are in the cloud. The network is secured and you patch once a month or whenever you think about it. You can map new devices and troubleshoot as needs arise. No big deal.

FACT: What you don't know about IT will eventually hurt you.

Every day, millions of automated scripts are running throughout the internet looking for access points. Email attachments, browser exploits, real and fake software updates, very convincing phishing campaigns, "free" downloads with default installation settings for malware and bloatware, and increasingly, social media exploits.

52% of data security breaches occur due to human error or system failure, rather than malicious intent.*

On a properly managed computer, an IT support system will scan thousands of data points every day looking for errors, countless entries in system logs, virus and malware alerts, Microsoft updates, third-party utility updates, and system capacity.

If an error goes unnoticed, it could result in a crashed system instead of a proactive fix. It is impractical for an individual person to stay up-to-date or to be proactive, given the volume of logs and updates that are generated every day.

Automation, monitoring and reliable response practices are a must.

Assumption #4: I haven't had a problem for years. Why should I worry about it now?

This rationale pops up frequently when users were active during the Y2K crisis. When all the dust settled, conventional wisdom held that the issue was mostly hype and we shouldn't have made such a fuss. That sentiment persists to the present day.

FACT: There is an exponentially greater number of threats today.

The Y2K crisis was in all likelihood a genuine threat, because the built-in date flaw was present in almost every type of software, in many solid-state devices, in every industry vertical, and especially so in government applications. Fortunately, high awareness and proactive effort paid off with minimal failures.

In 2017, systems are increasingly complex, there are more regulations to be aware of, your data is more critical than ever, and the burden of anticipating and mitigating threats is far heavier.

60 percent of small companies go out of business within six months of a cyber attack.*

Not only do you need the insurance, but also examining your security and IT management procedures can have the side effect of improving IT performance – something that companies who anticipated and headed off the “millennium bug” realized.

Assumption #5: It’s too expensive.

Right now, you may be weighing the cost of outsourcing management of IT support against the cost of “doing nothing.” While the cost of a service agreement is a fraction of hiring a full-time dedicated IT administrator, it still might feel like an “optional” expense that could be among the first line items to go.

FACT: Your information technology is a critical asset and represents the cost of doing business. It is the lever that can either stunt your growth if poorly managed, or allow you to multiply your efforts beyond your current capacity.

It may seem trite, but the question shouldn’t be, “Can I afford professionally managed IT?” but rather, “Can I afford NOT to have professionally managed IT?”

Try scratching out some numbers: what is an hour of downtime worth? In the event of a compliance violation, what fines might you be subject to? Can your business survive a catastrophic data loss? Can you withstand a lawsuit if your network infects another network?

Managed IT services are a proactive way to safeguard your data, your productivity and your business from unseen threats or normal failures. It is the cost of doing business today.

Bonus! Assumption #6: Only bigger companies have time to keep track of print utilization.

One of the most common neglected areas of management is printing and copying costs. You look at the small number of multi-function copier-printers combined with a dozen laser desktop printers, perhaps even a handful of inkjets, and think, “This isn’t worth managing.”

51% of surveyed small businesses are not allocating any budget to risk mitigation.*

FACT: Print usually represents the third largest business expense after payroll and facility costs.

You probably look closely at every lease you sign and you carefully plan capital projects. You’re cautious about screening employee and vendor candidates and you balance expenses and costs against opportunities. Are you missing an opportunity to manage print costs, which could be as high as 3% of your revenue?

Not only does managing your print volume and operational costs give you good intelligence about where printing is occurring, it can also help you streamline your fleet of printers through better placement, higher utilization, and replacing unreliable devices with reliable ones.

Effective managed print services reduce costly company downtime resulting from printer issues. An hour of printer-copier downtime for a 50-person company may have a proportionately much bigger impact than an hour of downtime for one department of a 1,000-person enterprise.

Ask Scantron for Recommendations

Keep your company running smoothly with a secure, highly performing and highly available IT environment. Contact STS to talk about developing an IT strategy that makes sense for your company. Leverage our industry-leading tools, experienced field service technicians and prompt remote and onsite service capabilities. Learn more at www.scantronts.com.